INFOSEC ฉบับ ต่อ จากฉบับที่แล้ว เรื่องสำคัญขององค์การในยุค Net Gen

วิชญ์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

สำหรับ INFOSEC นั้น ผู้เขียนเคยนำเสนอในบทความ “Information Security Awareness เรื่องสำคัญที่ไม่ควรมองข้าม” INFOSEC ดำเนินการเพื่อเป้าหมาย 3 ประการคือ

1) Confidentiality เพื่อรักษาความลับของข้อมูลหรือสารสนเทศสำคัญที่อาจส่งผลกระทบต่อการดำเนินงานขององค์การ

2) Integrity เพื่อรักษาข้อมูลหรือสารสนเทศสำคัญให้อยู่ในสถาพสมบูรณ์ไม่ถูกแก้ไขเปลี่ยนแปลง หรือบิดเบือนจากความจริง เพื่อสร้างให้เกิดความน่าเชื่อถือของข้อมูล และความเชื่อมั่นจากผู้ที่นำไปใช้งาน

3) Availability เพื่อให้ระบบข้อมูล หรือระบบสารสนเทศมีความพร้อมในการใช้งาน พร้อมให้บริการอยู่เสมอไม่ถูกทำให้ต้องหยุดการให้บริการซึ่งอาจส่งผลกระทบต่อความน่าเชื่อถือ และทำให้การดำเนินงานขององค์การหยุดชะงัก

ด้วยเป้าหมายในการรักษาความมั่นคงปลอดภัยของข้อมูลและสารสนเทศข้างต้น ทำให้คนส่วนใหญ่จะมอง INFOSEC ในมุมของการป้องกันการถูกคุกคามหรือโจมตีจาก Malicious Software ที่เรารู้จักกันในชื่อของ Malware ซึ่งมีอยู่หลากหลายประเภท เช่น Virus Spyware Adware Trojan Horse ฯลฯ บางประเภทถูกนำมาใช้เป็นเครื่องมือของผู้ที่ไม่ประสงค์ดีจำพวก Hacker Cracker โดยจะทำการโจมตีผ่านระบบ Network และที่สำคัญคือเข้าถึงผ่านเครือข่าย Internet แต่ในที่นี้จะไม่รวมถึงการหลอกลวงจำพวก Phishing Pharming ที่เป็นการปลอมแปลง Website แก้ไขระบบ DNS เพื่อหลอกลวงเอาข้อมูลทางธุรกรรม และการเงินจากเหยื่อ เพราะเป็นความเสี่ยงที่เกิดจากความผิดพลาดของบุคคลที่เป็นเหยื่อ ซึ่งสามารถแก้ไขโดยดำเนินการควบคุมในเชิงนโยบาย หรือข้อแนะนำในการใช้งานระบบสารสนเทศ และเครือข่ายได้ รวมถึงข้อมูลที่เสียหายส่วนใหญ่จะเป็นข้อมูลส่วนบุคคลไม่ค่อยส่งผลกระทบต่อองค์การในภาพรวม ยกเว้นกรณีที่ถูกหลอกลวงผ่านการเชื่อมต่อเครือข่าย Internet ขององค์การ ซึ่งอาจเกิดช่องโหว่ขึ้น และนำไปสู่การโจมตีแบบต่อเนื่องหลากหลายรูปแบบ

ปัจจุบันผู้บริหาร และผู้รับผิดชอบดูแลในเรื่อง INFOSEC ขององค์การที่พึ่งพาการนำเอาเทคโนโลยีสารสนเทศ และการสื่อสารมาใช้สนับสนุนการดำเนินงานอย่างเต็มรูปแบบ มีทางเลือกในการดำเนินการหลายหลายวิธี และส่วนมากหากองค์การมีการ Outsource งานด้านดังกล่าวก็จะเลือกใช้บริการของ Vendor หรือ Provider ที่ดูแลโดยการทำสัญญาผูกพันความรับผิดชอบต่อความเสียหาย และระดับการให้บริการ (Service Level Agreement: SLA) โดยเฉพาะ

การดำเนินการในด้านเทคนิคเพื่อป้องกันการโจมตีจากภายนอก สำหรับองค์การเองก็มีหน้าที่กำกับดูแล และควบคุมเชิงนโยบายกับบุคลากรขององค์การ เพื่อลดความเสี่ยงด้วยมาตรการต่างๆ ตามความเหมาะสม สิ่งสำคัญคือองค์การเองต้องมีความเข้าใจถึงประเด็นในการควบคุม ซึ่งในความเป็นจริงแล้วสามารถเริ่มต้นจากแนวคิดง่ายๆ เช่น

1. สิ่งสำคัญที่องค์การใช้ในการดำเนินงาน คือ ข้อมูลที่มีการจัดเก็บในระบบ Computer หากถูกทำให้ผิดพลาด สูญหาย หรือมีการลักลอบเอาไปให้คู่แข่งอาจเกิดความเสียหายต้องได้รับการปกป้อง

2. ระบบ Computer ที่ใช้ในการจัดเก็บข้อมูลสำคัญขององค์การนั้น มีอยู่ด้วยกันกี่ระบบ ติดตั้งเพื่อใช้งานหรือให้บริการบนเครือข่ายองค์การในส่วนใด สามารถเข้าถึงได้จากกี่ช่องทาง ได้รับการปกป้องมากน้อยแค่ไหน เหมาะสมหรือไม่

3. บุคลากรที่ทำหน้าที่ดูแลรับผิดชอบระบบข้อมูลคือใคร เป็นบุคลากรในองค์การ หรือใช้บริการของ Outsource และมีการกำกับควบคุมที่ดีแค่ไหน อย่างไร

หากองค์การมีความเข้าใจคำถามในพื้นฐานเหล่านี้ และได้ดำเนินการเพื่อลดความเสี่ยง หรือสามารถรู้เท่าทันสถานการณ์ได้อย่างเหมาะสมโดยอาจจะอยู่ในรูปแบบของนโยบาย หรือมาตรการในการกำกับการใช้งานแล้วหล่ะก็ ถือว่าสามารถควบคุมปัจจัยภายในได้ระดับหนึ่ง

อีกประเด็นที่สำคัญ คือ การควบคุมการเข้าถึง (Access Control) สำหรับผู้ใช้งานทั้งที่เป็นบุคลากรขององค์การเอง หรือบุคคลภายนอกที่ได้รับอนุญาต รวมถึงผู้ไม่ประสงค์ดี ซึ่งแค่การดำเนินการด้านนโยบายนั้นไม่สามารถที่จะกำกับควบคุมได้ จำเป็นต้องดำเนินการด้านเทคนิคเพื่อควบคุมการเข้าถึงข้อมูล หรือระบบสารสนเทศสำคัญควบคู่กัน

นอกเหนือจากการควบคุมในมิติของเครือข่ายสารสนเทศ หรือ Network แล้ว การดำเนินการเรื่อง Access Control ถือเป็นเรื่องที่สำคัญอย่างยิ่ง เพราะเป็นการดำเนินการที่ตรงไปตรงมา กล่าวคือ ใครสามารถเข้าถึงข้อมูลหรือระบบสารสนเทศสำคัญขององค์การได้บ้าง และใช้วิธีการใดในการเข้าถึง ซึ่งเหล่านี้เกี่ยวข้องกับการยืนยันตัวตนของผู้ที่ได้รับสิทธิ์ในการเข้าถึง (Authentication) และเข้าถึงได้ในระดับใด (Authorization) ในหลักการสากลนั้น กลไกการยืนยันตัวตนของบุคคลที่ได้รับสิทธิ์จะเลือกใช้จาก 3 ปัจจัย หรือใช้ร่วมกันในรูปแบบต่างๆ ปัจจัยหรือ Factor ทั้ง 3 นั้นคือสิ่งที่บุคคลที่ได้รับสิทธิ์ รู้ มี และเป็น ได้แก่

1. Something you Know อาทิ Password
2. Something you have อาทิ Smart Card RFID Card
3. Something you are อาทิ Biometric เช่น ลายนิ้วมือ ม่านตา เสียง เป็นต้น

ปัจจุบันมีหลายองค์การนำ Factor ทั้ง 3 มาใช้งานแบบผสมผสานได้อย่างเหมาะสมกับความสำคัญของข้อมูล หรือระบบสารนเทศที่ต้องการปกป้อง

ความเข้าใจในหลักการ และประเด็นเหล่านี้เป็นพื้นฐานที่สำคัญขององค์การที่พึ่งพาเทคโนโลยีสารสนเทศ และการสื่อสารในการดำเนินงาน และต้องการปกป้องข้อมูลสำคัญ เพื่อที่จะสามารถดำเนินการได้อย่างเหมาะสมตรงประเด็น และเกิดประโยชน์มิใช่เพียงพึ่งพาผู้ให้บริการ หรือบุคลากรเพียงบางกลุ่มแต่ไม่สามารถกำกับดูแลได้อย่างมีประสิทธิภาพ ส่งผลให้เกิดการดำเนินงานที่มีความเสี่ยง รวมถึงลงทุนที่มากเกินความจำเป็น ข้อสำคัญคือองค์การต้องเริ่มจากการตั้งคำถามบนความต้องการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศสำคัญก่อน เพราะการตอบคำถามเหล่านั้นจะนำไปสู่การดำเนินการที่เหมาะสม โดยอาจไม่จำเป็นต้องเข้าใจงานด้านเทคนิคว่าต้องใช้อุปกรณ์อะไรบ้าง ใช้เทคโนโลยีอะไร เข้ารหัสข้อมูลด้วย Algorithm อะไร แต่ต้องสามารถกำหนดกระบวนการควบคุม รวมถึงมาตรการบังคับใช้ที่เป็นรูปธรรมได้เพื่อใช้เป็นเครื่องมือในการกำกับดูแลที่มีคุณภาพ

โดยสรุปแล้ว องค์การควรมุ่งเน้นไปที่ที่ความต้องการ และความจำเป็นในการรักษาความมั่นคงปลอดภัยข้อมูลซึ่งอาจมีเพียงไม่กี่ประเด็นเท่านั้น แทนการมองไปยังเทคโนโลยีที่มีความสามารถสูง ใช้งานสะดวก และทันสมัย เพราะแม้ว่าเครื่องมือจะดีมากเท่าใดก็ตาม แต่ก็อาจไม่เหมาะสมกับการนำมาใช้งานในองค์การ หากไม่พร้อม และไม่เกิดการยอมรับรวมถึงอาจกลายเป็นภาระ และอาจนำมาซึ่งความเสี่ยงในมิติที่องค์การคาดไม่ถึงก็เป็นได้

นอกจากนี้ความเข้าใจในความต้องการขององค์การจะสามารถตีกรอบการดำเนินงานให้แคบลงโดยเฉพาะการดำเนินงานเพื่อจัดทำนโยบายในการกำกับควบคุม เพราะองค์การส่วนใหญ่หากต้องดำเนินการเรื่องจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศแล้วจะชอบหยิบยกเอารูปแบบหรือมาตรฐานสากลมาจับโดยไม่ได้ทำการศึกษาความต้องการให้ถ่องแท้ และเหมาะสมเสียก่อน เกิดเป็นการดำเนินงานแบบหว่านแห โดยเฉพาะการนำเอา ISO/IEC 27000 Series ได้แก่ ISO27001 และ 27002 มาพัฒนานโยบายด้านความมั่นคงปลอดภัยสารสนเทศซึ่งครอบคลุม 11 Domain หลัก และมีแนวทางดำเนินงาน Best Practice ที่มาจากองค์การในต่างประเทศ ซึ่งอาจไม่เหมาะสมกับองค์การ และอาจไม่สามารถตอบโจทย์ความต้องการขององค์การได้ในบางประเด็นที่มีความสำคัญ ที่แน่ๆ คือ องค์การต้องลงมือ ลงแรงศึกษาวิเคราะห์มาตรฐานสากลดังกล่าวเพื่อปรับใช้กับองค์การ การจัดตั้งทีมงาน และอาจหมายรวมไปถึงการจัดจ้างที่ปรึกษาผู้เชี่ยวชาญ ทั้งที่ในบางกรณีมีแต่องค์การเท่านั้นที่เข้าใจและสามารถดำเนินการได้ด้วยตนเอง

INFOSEC เป็นเรื่องที่ไม่ควรมองข้ามขององค์การในยุค Net Gen หรือ Internet Generation ที่ข้อมูลข่าวสารมีความสำคัญ และเกิดขึ้นในทุกๆ เสี้ยววินาที การเข้าถึงข้อมูลทำได้โดยสะดวกรวมเร็ว และหลากหลายรูปแบบ ส่งผลให้การปกป้องข้อมูลสารสนเทศขององค์การกลายเป็นเรื่องที่มีความสำคัญพอๆ กับการใช้ประโยชน์จากข้อมูลดังกล่าวในการดำเนินงานขององค์การนั่นเอง TPA news